REMARKS

Claims **1-118** are pending in the application.

Claims **1-118** stand rejected.

Claims **1-5, 9-11, 23, 27-28, 30, 33-37, 39-54, 64, 68-73, 83, 87-90, 96-99, 101, 104** and **112** have been amended.

Claims **38, 57, 76** and **94-95** have been cancelled.

Formal Matters

Please note that on December 8, 2008, an Information Disclosure Statement was submitted. However, the Office Action does not include a copy of the submitted form PTO 1449 indicating that the references have been considered. Consequently, the applicant respectfully requests the Examiner to forward a copy of the submitted form PTO 1449 indicating that the references have been considered. If the Examiner has not received the IDS and PTO 1449, the Examiner is requested to telephone the undersigned.

Claim Objections

Claims 1, 18, 33, 52, 54, 55, 56 and 94, as well as the claims generally, are objected to for informalities. With regard to the objections to claims 1, 18, 33, 52, 54, 55, 56 and 94, among other such claims, the Office Action posits that certain of the recited elements (to wit, "first security level information," "second security level information" and "third security level information") must be introduced using an article (i.e., "a" or

"an"). While Applicant appreciates the Examiner's diligence in reviewing the claims, Applicant respectfully disagrees.

Applicant agrees that, in general, singular claim elements are to be introduced using an article. However, such introduction should not be made in that manner, if to do so would be grammatically incorrect. Thus, in the same manner that one would not refer to "an information," Applicant respectfully submits that the claim language in question should not be so amended. Applicant further respectfully note that, having properly introduced these elements, subsequent recitation of these claim elements maintains proper antecedent basis through the accepted use of the article "said." Applicant therefore respectfully submits this objection to independent claims 1, 33, 52, 71, 90 and 104, as well as certain of their dependent claims, is overcome.

Rejection of Claims Under 35 U.S.C. § 101

Claims 52-74 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant has amended the Specification to address the Examiner's concerns, and respectfully submits that this rejection is overcome thereby.

Rejection of Claims Under 35 U.S.C. § 102

Claims 1-118 stand rejected under 35 U.S.C. § 102(b) as being unpatentable by Williams, U.S. Patent No. 6,304,973 (Williams).

While not conceding that the cited references qualify as prior art, but instead to expedite prosecution, Applicant has chosen to respectfully disagree and traverse the rejection as follows. Applicant reserves the right, for example, in a continuing application, to establish that the cited reference, or other references cited now or hereafter, do not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed.

Applicant respectfully submits that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegall Bros. V. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Applicant respectfully submits that the Office Action fails to demonstrate that the reference shows, teaches or even suggests several of the claimed limitations. Independent claim 1, as amended, is representative of amended independent claims 33, 52, 71, 90 and 104, and now recites:

1. A method comprising:

comparing first security level information and second security level information, wherein

said first security level information represents a first security level,

said second security level information represents a second security level,

said first security level information is stored in a security label of a packet received at a network node of a network,

said second security level information is stored at said network node, after being received from another network node of said network,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said another network node, and

said network nodes are configured to convey packets to one another via others of said network nodes; and

indicating processing to be performed on said packet based on said comparing, wherein

said processing comprises

determining whether to forward said packet from said network node to one of said network nodes.

(Emphasis supplied)

As will be appreciated, independent claims 33, 52, 71, 90, 104 and 112 have been amended to recite comparable limitations. It will be further appreciated that certain of the amendments presented herein are editorial in nature, and merely reflect changes in wording and the like, rather than changes in substance.

By contrast, Williams is directed to:

"A network prevents unauthorized users from gaining access to confidential information. The network has various workstations and servers connected by a common medium and through a router to the Internet. The network has two major components, a Network Security Center (NSC) and security network interface cards or devices. The NSC is an administrative workstation through which the network security officer manages the network as a whole as well as the individual security devices. The security devices are interposed, between each of workstation, including the NSC, and the common medium and operate at a network

layer (layer 3) of the protocol hierarchy. The network allows trusted users to access outside information, including the Internet, while stopping outside attackers at their point of entry. At the same time, the network limits an unauthorized insider to information defined in their particular security profile. The user may select which virtual network to access at any given time. The result is trusted access to multiple secure Virtual Private Networks (VPN), all from a single desktop machine." (Williams, Abstract)

Applicants maintain that Williams fails to teach the limitations of the independent claims, as Williams is directed to the use of separate, individual security devices. The integrated approach of the claimed invention are simply not taught by Williams. For example, Williams is not concerned with the integration of security in network devices, but merely stand-alone devices analyzing network traffic to and from and single node, among other distinctions.

In order to highlight this distinction, Applicant has amended the independent claims as noted above. As can be seen in the amended independent claims, the claimed network node receives the second security level information from another of the nodes in the network, and then makes a determination as to whether to forward the received packet to one of those nodes (which may, in fact, be the nodes from which the second security level information was received), based on a comparison of the first security level information (from the packet) and the second security level information (as received from another network node and stored at the network node). Further, the claimed network

nodes (including the network node and another network node) are each configured to convey packets to one another via others of the network nodes.

Notwithstanding other inapposite parallels that would need to be drawn to successfully equate Williams' security device and the claimed invention, even if such were the case, Williams' security device would still be incapable of anticipating (or making obvious) the claimed invention, at least because Williams fails to show, teach or suggest any security device that receives any security information from a network device that is configured to convey packets to other such network nodes via other such network nodes. Furthermore, Williams' security device in simply not configured to convey packets to other such security devices via still others of such security devices.

In fact, Williams specifically eschews any such access. Williams definitively states:

> **"A key architectural feature of this hardware design is that the network medium 68 is separated from the host bus 42.** This separation of the two interfaces dictates that packets will move from one interface to the other only if moved by security device's 40 software 52. The only way a packet may move from host bus 42 to local bus 46, is for the CPU 48, running the firmware 52, to grab the packet from the two-port RAM 44.
>
> **In addition, the hardware design provides a separation of the security device's own processing environment from both the host and the network.** The security device's program and internal buffers are

invisible to the host because of the dual-ported RAM design. Further, except for control requests from the NSC 12, which are accepted only from the NSC and must be cryptographically verified, **there is no interface by which another host on the network can retrieve data from the security device's internal buffers**.

Because all communications from one host to another must use the services provided by the security device in order to access the network, it is not possible for a host to inadvertently or maliciously bypass the security device security features. In a properly configured network, where there are no other electrical connections to the network, it is possible to make absolute statements that the host software (whether trusted to operate in MLS mode, or not) must operate in accordance with the centralized network security policy set up by the security policy defined by the security officer at the NSC. Further, any packets that are transmitted are cryptographically protected before being placed on the network.

The security device functions are implemented in firmware 52 installed on the security device board. **During installation, the security device firmware reads an administrator installation card at the authentication interface unit 62 to get the board IP addresses (Node, NSC, default router) and cipher key. Subsequently, the security device downloads principal-specific and node-specific data, via the network interface 66, from the NSC and sends audit events to the network for**

archival. However, the security device operates independently of the attached host.

The security device has four general phases of operation: configuration, initialization, key exchange, and secure communication. Configuration is performed by the network security officer at the NSC workstation. The NSO configures each security device to support one or more principals, where each principal may have up to about 100 profiles. Each profile has associated mandatory access controls (security windows) and discretionary access controls (association lists).

Initialization of the security device occurs when a principal authenticates, via the security device, to the NSC. The security device reads security profile selected by the principal and cryptographic seed keying material from the database resident on the NSC. Whenever the security device establishes initial contact with another host that is also equipped with a security device, key exchange is conducted to prepare for secure communications between the hosts." (Williams, col. 20, ll. 11-50; Emphasis supplied)

As can be seen, then, even if the security device of Williams could somehow be successfully equated to the claimed network node (a point Applicant does not concede), the idea of one of Williams' security devices receiving something even remotely akin to the claimed security level information is not only foreign, but antithetical to the policies and philosophy espoused in Williams. Moreover, notwithstanding the failings of such an

attempted comparison, it is evident that Williams fails to show, teach or suggest receiving such information from any sort of network device, where such a network device is configured to convey packets to other such network devices via such network devices. Again, such functionality would be clearly antithetical to Williams stated purpose, and the functionality described therein.

While such distinctions are evident in the independent claims, Applicants have amended claim 2, as an example of such dependent claims, to further distinguish the claimed invention over Williams. Claim 2 now recites that:

> "...
> said another network node is coupled to a destination of said packet, and
> said destination is assigned said second security level.
> ..."

In the manner that receiving any manner of security information from another security device would be antithetical to Williams teachings, it is clear that receiving such information based on the destination of a packet is not only contrary to Williams philosophy, such a process is far beyond anything even contemplated by Williams (whether supported or eschewed thereby).

Applicant respectfully submits, therefore, that independent claims 1, 33, 52, 71, 90, 104 and 112 are allowable over Williams, and so Applicant respectfully urge that the §102 rejection of claims 1, 33, 52, 71, 90, 104 and 112, and claims depending thereon, be withdrawn.

CONCLUSION

In view of the amendments and remarks set forth herein, the application and the claims therein are believed to be in condition for allowance without any further examination and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned.

If any extensions of time under 37 C.F.R. § 1.136(a) are required in order for this submission to be considered timely, Applicant hereby petitions for such extensions. Applicant also hereby authorizes that any fees due for such extensions or any other fee associated with this submission, as specified in 37 C.F.R. § 1.16 or § 1.17, be charged to Deposit Account 502306.

I hereby certify that this correspondence is being submitted to the U.S. Patent and Trademark Office in accordance with 37 C.F.R. § 1.8 on November 9, 2009 by being (a) transmitted via the USPTO's electronic filing system; or (b) transmitted by facsimile to 571-273-8300; or (c) deposited with the U.S. Postal Service as First Class Mail in an envelope with sufficient postage addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia, 22313-1450.

/ Samuel G. Campbell, III / November 9, 2009

Samuel G. Campbell, III Date

Respectfully submitted,

/ Samuel G. Campbell III /

Samuel G. Campbell III
Attorney for Applicant(s)
Reg. No. 42,381
512-439-5084
512-439-5099 (fax)